МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ГЛОБАЛЬНОЕ УПРАВЛЕНИЕ ИНТЕРНЕТОМ: ВЗГЛЯД РОССИЙСКИХ И МЕЖДУНАРОДНЫХ ЭКСПЕРТОВ НА ВСТРЕЧЕ В ЖЕНЕВЕ

Первые 12 лет XXI в. были отмечены революционными изменениями в результате невероятно быстрого развития информационных и телекоммуникационных технологий (ИКТ), и в первую очередь интернета. Изменения затронули практически все пласты общественных процессов, включая международные отношения — от социальных и политических преобразований в арабском мире (Арабская весна) до беспрецедентного роста таких феноменов, как политически мотивированный хактивизм, слив государственных секретов в Сеть (Wikileaks), кибервойны и кибершпионаж. В то же время нарастает глобальная озабоченность вопросами предотвращения (либо победоносного ведения) войн в киберпространстве. Интернет и его эволюция не просто определяют все эти процессы, но и лежат в их основе. В связи с трансграничным характером глобальной сети последствия ее трансформации распространяются на всю планету. В процессе кардинальных преобразований сегодня находится вся архитектура глобального управления интернетом. Настоящая революция разворачивается и на третьем уровне интернет-архитектуры — на уровне пространства доменных имен DNS. Отдельным вопросом является регулирование транснациональных социальных сетей. Однако на данный момент ни один из этих вопросов не решается в рамках всеобщей, гармонизированной и всесторонней международной системы регулирования или хотя бы в рамках международного сотрудничества, способного закрыть все существующие пробелы и преодолеть проблемы, возникающие в данной области.

Анализ этих фундаментальных тенденций с использованием совместного и сбалансированного подхода всего международного сообщества требует широкого участия международных экспертов. Цели диалога состоят в выработке общих позиций в международном экспертном сообществе и формулировании совместной российской и европейской повестки дня по данным вопросам на неправительственном уровне. ПИР-Центр попытался положить начало подобному международному диалогу: 26 апреля 2012 г. в Женеве состоялось совместное расширенное заседание Международного клуба Триалог и европейского отделения ПИР-Центра, Centre russe d'etudes politiques.

*Заседание открыл президент ПИР-Центра Владимир **Орлов**. Главный доклад круглого стола был представлен председателем правления ПИР-Центра Михаилом **Якушевым**. В заседании участвовали: глава Программы по новым угрозам безопасности Института ООН по исследованию проблем разоружения Бен **Бейсли-***

***Уокер**, директор отделения общественной политики ISOC Констанс **Боммелер**, заместитель постоянного представителя Российской Федерации в ООН и других международных организациях в Женеве Виктор **Васильев**, профессор гражданского, коммерческого и европейского законодательства Цюрихского университета Рольф **Вебер**, вице-президент Международного Общества Интернет (ISOC) Маркус **Куммер**, советник по стратегическим и политическим вопросам Отдела корпоративной стратегии Международного союза электросвязи Ярослав **Пондер** и заместитель постоянного представителя США на Конференции по разоружению в Женеве Уолтер **Рид**.*

ВЛАДИМИР ОРЛОВ (ПИР-ЦЕНТР): ПИР-Центр развивает проект в области глобального управления интернетом и международной информационной безопасности, пытаясь обобщить и довести до наших партнеров видение этих проблем из России. Здесь существует большое количество проблемных областей, в том числе *облачные* компьютерные системы и их безопасность; идентификация в интернете; использование социальных сетей. Иногда у меня складывается впечатление, что мы рискуем утонуть в огромном потоке тем, сконцентрированных *под шапкой* нашего проекта. Конечно, существует множество юридических проблем — например, связанных с неучастием России в Будапештской конвенции *О киберпреступности* и в других *жестких* и *мягких* законодательных механизмах, направленных на эффективную борьбу с трансграничной киберпреступностью. В этой связи ПИР-Центр ставит перед собой задачу охватить все многочисленные грани этой проблематики, начиная с юридических и технических аспектов и заканчивая выработкой практических рекомендаций для лиц, принимающих решения в РФ, и их ключевых зарубежных партнеров.

В сферу интересов ПИР-Центра входит весь спектр данной проблематики, однако основное внимание уделяется, конечно же, вопросам, лежащим в плоскости практической политики. Как повлиять на политический курс? Как можно и необходимо скорректировать его, для того чтобы он отражал реальную ситуацию и учитывал текущие глобальные процессы? Именно на этих вопросах мы хотели сконцентрироваться, когда запускали наш проект.

А сейчас давайте приступим к самому первому заседанию в широком составе, которое в определенном смысле также является частью этого проекта. Я бы хотел, чтобы сегодня мы обсудили такие ключевые вопросы, как трансформация архитектуры интернета и системы управления Сетью; новая повестка дня в области международной информационной безопасности и ключевых проблем киберпространства и, конечно же, роль России во всех этих вопросах глобального порядка.

АРХИТЕКТУРА ИНТЕРНЕТА И УРОВНИ УПРАВЛЕНИЯ ИНТЕРНЕТОМ

МИХАИЛ ЯКУШЕВ (ПИР-ЦЕНТР): Прежде всего я бы хотел отметить различия в определениях и терминологии вопроса, который мы сейчас обсуждаем. В русском языке и российской дипломатии в основном используются термины, которые отличаются от широко распространенных на международном уровне понятий *управление интернетом* [*internet governance*] и *кибербезопасность* [*cyber security*]. Вместо этого Россия развивает и продвигает концепцию *информационной безопасности* [*information security*] — в нашей стране наиболее широко используется именно этот термин. Фактически мы говорим об одних и тех же явлениях и проблемах, однако обозначаем их разными словами, поэтому нам следует попытаться понять друг друга и постараться говорить на одном языке.

Управление интернетом имеет множество разных аспектов, и в этом смысле оно не отличается от любого другого комплексного аспекта международной безопасности. Когда мы ведем речь об освоении космоса и связанных с ним юридических

и политических вопросах, нам следует принимать во внимание принципы космической деятельности, включая принцип ответственности, прав и обязанностей запускающих космические аппараты государств, правовой статус Луны и других небесных тел и т.д. Когда мы говорим об атомной энергии, нам нужно иметь в виду проблемы контроля над вооружениями, нераспространения, военного и мирного использования ядерных материалов, ответственность ядерных операторов и другие подобные вопросы. То же самое относится и к интернету — невозможно дать короткие и точные ответы на вопросы о том, что делать в сфере управления интернетом, кто несет ответственность за это управление и какие договоры или конвенции следует разработать, чтобы закрыть пробелы и найти решение всем существующим проблемам.

Более того, когда заходит разговор об интернете, мы иногда говорим об абсолютно разных вещах, которые в своей совокупности образуют понятие «интернет». Сюда входит техническая инфраструктура, каналы телекоммуникаций и различные типы оборудования, которые обеспечивают доступ к сети. Сетевая инфраструктура радикально отличается от той системы, которую мы имели в эпоху *традиционных* телекоммуникаций, таких как телеграф или телефон. Наконец, говоря об уровне практического использования интернета, следует учитывать, какую важность приобрела глобальная сеть, особенно в связи с колоссальными достижениями в ее развитии и проникновении в мире.

Однако даже на уровне инфраструктуры существуют различные подуровни, которые регулируются различными организациями в соответствии с самыми разными принципами. В понятие инфраструктуры Сети входят волоконно-оптические кабели, спутниковые каналы, радиочастотный спектр и т.д. Сюда же относятся такие вопросы, как так называемые *проблемы последней мили*, а также различные типы оборудования для доступа, пользовательского оборудования и оборудования на площадке клиента интернет-сервисов. В данной сфере применяются совершенно другие принципы регулирования, если речь идет, например, о станциях спутниковой связи.

То же можно сказать и о самой сетевой архитектуре, которая весьма разнообразна в техническом, организационном и регуляторном плане. Говоря о сетевой архитектуре, следует учитывать различные ее уровни, начиная с уровня корневых серверов — речь идет о знаменитых корневых серверах, которые расположены в разных странах мира; они представляют собой *ядро* интернета. Нужно также учитывать вопросы, связанные с развитием системы IP-адресации: в настоящий момент мы наблюдаем переход с предыдущей версии IP-протокола, *IPv4*, на новую версию, *IPv6*. Этот переход будет означать значительное изменение всей архитектуры интернета. Фактически интернет превращается из *сети людей* в *сеть предметов* — собственные IP-адреса смогут получить — и уже получают — наши холодильники, автомобили и различные электронные устройства, приобретающие способность обмениваться информацией.

Третьим уровнем сетевой архитектуры является система доменных имен, которая связана с геополитикой. К настоящему моменту сложилась система так называемых доменов верхнего уровня, соответствующих коду страны и определенным образом отражающих принцип государственного суверенитета. Однако в 2012 г. начали внедряться нововведения, согласно которым количество доменов верхнего уровня увеличивается до нескольких сотен или даже тысяч. Например, становятся возможным такие домены верхнего уровня, как *.microsoft*, *.Facebook*, *.google*, *.religion*, *.luckilyman,* то есть благодаря этому гениальному нововведению становится возможным создать и ввести в использование практически любое доменное имя. Многие обыватели, управленцы и даже эксперты пока не понимают, сколь масштабные изменения предстоят в этой связи в ближайшее время и как эти изменения отразятся на всех нас.

Наконец, на уровне практических приложений существует огромное количество вебсайтов. Их число уже исчисляется миллиардами; они регулируются различными способами и по законодательству разных юрисдикций, но с помощью них мы понимаем, что происходит в интернете — и это именно то, для этого существует и используется интернет. Однако сам по себе вебсайт должен регулироваться, так же, как это происходит со средствами массовой информации. В разных странах СМИ регулируются независимо от того, являются ли они онлайновыми или оффлайновыми, и это очень важный вопрос в контексте распространения информации и развития массовых коммуникаций. Скоро уже не будет проблемой найти в интернете любую информацию, вовсе не используя систему доменных имен. Это можно сделать с помощью таких поисковиков, как *Google* или *Yandex*. К примеру, если вы хотите узнать, что такое *Centre russe d'etudes politiques*, который является организатором нашей сегодняшней встречи, совсем не обязательно запоминать название этой организации в швейцарском домене *.ch*. Достаточно ввести его или название любой другой организации в поисковик, и с вероятностью 100 % поисковая машина выведет вас на нужный интернет-ресурс. При этом не играет никакой роли, где именно данный ресурс расположен.

Особенно большие возможности в сегодняшнем интернете предлагают социальные сети, в частности потому, что практически никак не регулируются. Большинство социальных сетей транснациональны, а их аудиторию составляют *юзеры* со всего мира. Количество пользователей *Facebook* недавно перевалило за 900 млн человек. Если бы аудитория сети Марка Цукерберга составляла население одной страны, то эта страна была бы третьей в мире по численности населения после Китая и Индии. Соответственно, возникают вопросы о том, кто должен регулировать деятельность пользователей *Facebook* и с какой регулирующей инстанцией должна взаимодействовать данная социальная сеть по вопросам, так или иначе затрагивающим проблематику обеспечения глобальной безопасности.

Еще одно новое измерение, которое сейчас активно развивается — это мобильное пространство интернет-коммуникации. Во многих странах — и Россия здесь не исключение — многие пользователи все чаще выходят в интернет не через традиционные компьютеры, а со своих мобильных телефонов, планшетов и других портативных устройств. Это тоже очень сильно меняет ландшафт интернета, поскольку уже сейчас есть некоторые приложения, которые не работают на обычном настольном компьютере — они адаптированы именно под портативные устройства. Поэтому нам также необходимо говорить об интеграции мобильных сетей и компьютерных сетей в интернете. В 2020 г. интернет будет сильно отличаться от сегодняшней глобальной сети, точно так же, как сегодняшний интернет сильно отличается от интернета пятнадцатилетней или даже десятилетней давности.

РОЛЬФ ВЕБЕР (ЦЮРИХСКИЙ УНИВЕРСИТЕТ): Относительно важности инфраструктуры ни у кого сомнений нет. Мы также понимаем, что сегодня дело приходится иметь с самой разнообразной инфраструктурой. Одного лишь анализа телекоммуникационных сетей для рассмотрения проблемы мало — нужно учитывать спутники, радиочастотный спектр, а также постоянно растущее количество мобильных телефонов. Что касается России, то, как уже сказал М. В. Якушев, в этой стране использование мобильных телефонов для доступа в интернет широко распространено, как и во многих других странах мира. Мне часто приходится работать в Восточной Азии, и во многих странах этого региона основным способом доступа в интернет уже стал именно мобильный телефон, а не компьютерные сети. Новые технологии также направлены на разрешение вопросов безопасности, и нам это следует учитывать.

Основным прародителем нынешней глобальной сети было американское Министерство обороны, то есть американские военные. Давайте вспомним сеть ARPANET, которая с течением времени все больше и больше развивалась в сто-

рону обслуживания гражданского и частного сектора с одновременным сокращением роли военных. Сегодня мне иногда даже кажется удивительным, что чем больше дискуссия сводится к вопросам обороны и безопасности, тем менее важной она начинает казаться в контексте общей проблематики развития интернета. Дискуссии на эту тему уже не представляются настолько значимыми, как в самом начале эпохи Сети, когда сам интернет и его техническая инфраструктура только начинали формироваться в обстановке холодной войны.

ОБЕСПЕЧЕНИЕ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ И УПРАВЛЕНИЕ ИНТЕРНЕТОМ

ЯКУШЕВ: Очень интересные дебаты разворачиваются сегодня вокруг принципа суверенитета государств. Сохраняет ли государство свой суверенитет в эпоху интернета или же концепция политического суверенитета трансформируется, размывается, превращаясь, к примеру, в концепцию *совместного суверенитета*? На этот вопрос очень трудно дать однозначный ответ. С одной стороны, существует широкое международное признание недопустимости вмешательства во внутренние дела любой страны. Никто не оспаривает право Китая, Ирана или арабских стран накладывать определенные ограничения на интернет, на доступ в интернет, или на распространение информации в Сети в пределах своей страны.

Однако есть также пример Ливии и Сирии, в ситуации с которыми со стороны международного сообщества и отдельных стран проявляют себя так называемые интересы гуманитарного вмешательства. Массовые нарушения прав человека в этих странах используются как предлог определенными странами или международными организациями, которые хотят изменить ситуацию и стремятся прекратить нарушения прав человека теми или иными способами. Появляются различные международные либо национальные документы, имеющие международные последствия, такие как, например, Международная стратегия по действиям в киберпространстве (2011 г.), которая излагает и фиксирует принципы поведения США в киберпространстве. Этот документ спровоцировал горячие дебаты по всему миру. Есть и предложения Российской Федерации, на которых я подробно остановлюсь чуть позднее. Однако на сегодняшний день, к сожалению, несмотря на ведущиеся дискуссии в рамках ООН, мы не видим перспектив для компромисса. К сожалению, вопросы, связанные с обеспечением международной информационной безопасности (МИБ) и глобальным управлением интернетом, в массе своей крайне политизированы. *Арабская весна* и революционные события в разных странах на фоне активной социальной самоорганизации в социальных сетях, ограничения на свободу слова и другие политически *чувствительные* процессы не дают нам возможности говорить о разработке документа, а точнее, международного юридического инструмента, который заполнил бы существующие пробелы и дал ответы на все эти вопросы. Однако в то же время вполне очевиден ряд проблем, в скорейшем разрешении которых заинтересованы все, с другой стороны, нет времени ждать, пока эти проблемы каким-то образом разрешатся сами собой.

Я бы хотел привлечь ваше внимание к решению, принятому Советом Европы, который объединяет почти все страны европейского континента и к чьим документам относятся с уважением не только в европейских странах, но и по другую сторону Атлантики — в Америке, Африке, в азиатских странах. В прошлом году, 21 сентября 2011 г., Комитет министров Совета Европы принял ряд очень важных документов, которые следует рассматривать в качестве элемента так называемого *мягкого права в области информационной безопасности*. Речь не идет о международном договоре или резолюции Совета Безопасности ООН, имеющих обязательную юридическую силу. Но поскольку Россия и большинство стран Европы являются членами Совета Европы, такие рекомендации и *мягкие* законодательные документы являются отличным примером возможного компромисса по определенным вопросам,

относящимся к управлению интернетом. Речь идет, в частности, о трансграничном ущербе и трансграничных последствиях действий государств. В этой связи Совет Европы принял декларацию Комитета министров о принципах управления интернетом, в которой были одобрены рекомендации для государств — членов СЕ в области защиты и развития всеобщего, целостного и открытого характера интернета.

Существует 10 принципов управления интернетом, общепринятых для всех европейских страна, включая страны — члены Совета Европы. К числу таких принципов относится, в частности, защита фундаментальных прав и свобод, а также повсеместное укоренение *мультистейкхолдерской модели* управления интернетом, то есть модели, предполагающей участие в процессе управления всех заинтересованных сторон.

Существует также принцип ответственности государств. Управление интернетом очень часто затрагивает права государств, и в этом смысле Совет Европы создал прецедент, установив принцип ответственности за предотвращение нанесения трансграничного ущерба — в том числе ущерба вследствие принятия определенных внутригосударственных законов и правил. Известен ряд примеров, когда внутренние решения или даже непреднамеренные действия на уровне одних государств наносили определенный ущерб другим государствам. К примеру, в 2011 г. одна женщина в Грузии умудрилась перерубить лопатой оптико-волоконный кабель, проходящий через ее деревню. В результате без доступа к Сети осталась вся Армения.

Что нужно сделать, чтобы не допустить повторения таких инцидентов? Я не собираюсь перечислять все 10 принципов, но некоторые из них все же стоит упомянуть. Девятый принцип гласит, что нельзя допускать никакого манипулирования интернет-трафиком. К примеру, нельзя наделять приоритетом определенные виды трафика. Кроме того, нельзя ограничивать доступ к определенным типам ресурсов по политическим или иным причинам, если такие меры не соответствуют требованиям международного законодательства по защите свободы слова и свободы доступа к информации. Очень важен десятый принцип — принцип культурного и языкового разнообразия, распространяющийся на виртуальное пространство глобальной сети.

Предпринимались неоднократные попытки выработать международный документ, который ответил хотя бы на некоторые открытые вопросы. В 2005 г. бывший генеральный секретарь ООН Кофи Аннан организовал в Женеве несколько заседаний Рабочей группы по управлению интернетом. Все члены рабочей группы были назначены самим генеральным секретарем. Окончательный отчет группы был опубликован в 2005 г. и содержал определенные конкретные решения, пояснения и параграфы, в рамках которых действительно была предпринята попытка дать ответ на некоторые из приоритетных вопросов в области глобального управления интернетом. Темы, затронутые в этом отчете, в настоящее время обсуждаются на заседаниях Форумов по управлению интернетом, которые проводятся ежегодно.

В других предложениях, вносимых такими странами, как США и Россия, фундаментальные принципы международного права должны стать неотъемлемой частью — иначе будет очень трудно защищать и продвигать на глобальной арене их основные идеи и положения. К примеру, если мы пытаемся предотвратить *кибервойну*, нужно одновременно работать над предотвращением незаконной деятельности интернет-пользователей, направленной против государства и общества (кибертерроризм), а также незаконные действия против других пользователей (т.е. киберпреступность). Стоит также вопрос о предотвращении незаконных действий правительств и группировок, действующих в их интересах, против интернет-пользователей.

ВЕБЕР: Конечно, один из ключевых вопросов — насколько и в какой степени нам вообще необходимо регулирование интернета. В самом начале, в 1996 г., Джон Перри Барлоу заявил в своей знаменитой Декларации независимости киберпространства, что нам вообще не нужно никакое регулирование, поскольку киберпространство является абсолютно отдельным миром, которому не нужны указки правительства или игроков частного сектора. Естественно, с тех пор взгляды на вопрос регулирования очень сильно изменились. Этот процесс привел, как очень хорошо и подробно нам рассказал М. В. Якушев, к появлению идеи управления интернетом с силами множества стейкхолдеров, то есть заинтересованных участников. У нас сейчас есть три основных столпа: правительства, частный сектор и гражданское общество. Однако существует и такой феномен: частный сектор и гражданское общество все больше концентрируются на таких аспектах, как система доменных имен, защита личной информации, права человека и цензура, несколько дистанцируясь от вопросов безопасности киберпространства.

Если посмотреть на список тем, обсуждаемых на Форумах по управлению интернетом (IGF) за последние шесть лет, становится очевидно, что вопросам кибертерроризма и киберпреступности, к примеру, уделяется очень мало внимания. Я не говорю, что эти вопросы вообще не обсуждаются, но нет сомнений, что такие дискуссии находятся на периферии внимания в рамках Форума IGF — по крайней мере, именно так обстояли дела на первых пяти форумах. Это на самом деле не так уж и удивительно, поскольку проблемы кибертерроризма и особенно кибервойн в основном решаются на уровне правительств, в то время как участники IGF в большей степени представляют гражданское общество. Так что, наверное, для участников этих форумов киберпреступность играет определенную роль, но намного больше их заботят другие проблемы. Именно поэтому, к примеру, обсуждение Конвенции Совета Европы *О киберпреступности* так долго не включалось в повестку дня IGF. При этом на заседаниях Корпорации по присвоению имен и номеров в интернете (ICANN) аспекты киберпреступности и кибербезопасности вообще не играли и до сих пор почти не играют никакой роли. Вместе с тем, международное сообщество, похоже, движется в направлении определенного компромисса. М. В. Якушев упомянул попытку Совета Европы решить вопрос о закреплении принципов управления интернетом. Правительства некоторых других стран — к примеру, Бразилии — также начали работу над формулированием принципов управления глобальной сетью. Предпринимаются попытки выработать что-то вроде *декларации о правах человека в интернете*. Подобная инициатива в настоящее время поддерживается компанией *Google* через один исследовательский институт в Берлине, которому с этой целью предоставляются довольно серьезные ресурсы.

Однако, как это ни удивительно, я пока не вижу особого внимания к вопросам национальной или международной безопасности в контексте киберпространства и в частности интернета. По моему мнению, эта сфера требует более пристального внимания. Решать эту проблему нужно уже в ближайшем будущем — более того, я бы даже сказал, что ее нужно решать срочно, пока не стало слишком поздно. Иными словами, акцент необходимо делать на мерах безопасности. Наконец, хотелось бы также упомянуть, что уже есть пара документов в этой области, которые можно использовать в качестве основы для дальнейшего обсуждения. К примеру, Организация экономического сотрудничества и развития (ОЭСР), которая хотя и не является всемирной организацией, но объединяет 34 государства в основном из числа развитых стран, в 2002 г. опубликовала свои рекомендации по информационной безопасности. Таким образом, опыт практических наработок ОЭСР в этой сфере насчитывает уже 10 лет и вполне может быть использован в качестве отправной посылки для дальнейшего обсуждения.

КОНСТАНС БОММЕЛЕР (**INTERNET SOCIETY**): Я бы хотела добавить несколько слов к тому, что сказал профессор Вебер. На международном уровне уже сейчас предпринимаются определенные усилия в области борьбы с киберпреступностью

и обеспечения безопасности киберпространства. Недавно Интерпол объявил о своей работе над созданием глобальной системы, которая позволит быстро идентифицировать авторов незаконных действий в киберпространстве. Я не знаю, насколько широко известны эти инициативы, но мне представляется, что первые определенные шаги в плане международного сотрудничества уже делаются. Конечно, работая над этими инициативами, нужно не забывать о нерешенных вопросах в плане неприкосновенности личной жизни и персональных данных, так что продвигаться в этом направлении следует осторожно. Но определенные усилия уже предпринимаются, и мы будем надеяться, что они дадут положительный результат.

ВЕБЕР: Я бы хотел прокомментировать по крайней мере пару заявлений и мыслей, высказанных М. В. Якушевым. Наверное, стоит начать с вопроса о том, как вообще подходить к проблеме регулирования интернета. Есть ли какая-то реальная необходимость в таком регулировании? Кто должен устанавливать правила? Чьи интересы должны быть защищены этими правилами, и нужны ли какие-то специальные механизмы? Если проанализировать последние 15 лет с тех пор, как была создана ICANN, то становится ясно, что теперь в управлении киберпространством принимает участие широкое сообщество и что это привело к очень интересным изменениям. Фактически произошел переход от централизованного регулирования к интересам отдельных государств и мультистейкхолдерской модели.

Кроме того, возвращаясь к темам, которые я уже затрагивал, я также считаю, что существует необходимость в усовершенствовании структуры ICANN. Что касается заявок на новую систему доменных имен DNS, в этой связи была зафиксирована серьезная проблема с безопасностью. Судя по всему, лица, подавшие заявки, могли получить несанкционированный доступ к информации, принадлежащей другим заявителям, которые уже загрузили свою информацию. Реакция ICANN на эту ситуацию была, на мой взгляд, недостаточно профессиональной. Фактически, представители ICANN лишь заявили, что делают все возможное для решения этой проблемы с безопасностью. Однако не последовало никаких четких рекомендаций относительно того, какие действия нужно было предпринимать. Осталось непонятно, кто отвечает за сложившуюся ситуацию в самой Корпорации. Отсутствовало даже четкое разделение сфер ответственности и, наконец, было невозможно применить правила об ответственности за ущерб, поскольку непонятно было, какой конкретно ущерб был нанесен в связи с утечкой информации. Описанная выше ситуация подтвердила потребность детально проанализировать глобальные аспекты безопасности интернета в рамках ICANN.

Мое предположение в этой связи сводилось к тому, что необходимо заложить прочную институциональную основу для управления ICANN, поскольку вопросы легитимности больше невозможно игнорировать. Я подал некоторые предложения относительно возможных путей устранения слабых мест в существующей системе. Я не говорю, что нужно искать замену Корпорации как таковой. Но я полагаю, что ICANN должна в большей степени учитывать широкие общественные интересы. И как специалист в области права, я не могу не отметить, что в настоящее время не существует даже нормальной системы для подачи апелляций на решения и действия Корпорации. Структура, которая необходима для придания баланса существующей системе, не должна представлять собой судебную инстанцию. Тем не менее существует явная потребность в некоем независимом органе для рассмотрения решений, принимаемых ICANN.

ЯРОСЛАВ ПОНДЕР (МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ): Кибербезопасность является ключевым компонентом Женевского плана действий и Тунисской повестки дня, которые предлагают механизм имплементации. МСЭ предпринимает необходимые меры, чтобы Глобальная программа в области кибербезопасности, вступившая в силу в 2007 г. с участием всех ключевых сообществ

стейкхолдеров, принесла желаемые плоды на глобальном уровне. Эта дискуссия также получила развитие на Всемирном саммите по информационной безопасности, который состоялся 14–18 мая 2012 г. Мы вступили в фазу подведения промежуточных итогов этих процессов и анализируем результаты саммита. На этой основе мы стараемся понять, что хотели бы увидеть государства-участники после 2015 г. в плане глобальных мероприятий и с какими ранее неизвестными факторами и проблемами мы можем столкнуться. Поэтому вклад со стороны сообщества стейкхолдеров имеет огромное значение для разрешения многих вопросов, которые упоминались сегодня в ходе дискуссии и стали предметом обсуждения на ряде сессий в ходе Всемирного саммита.

Форум — не просто площадка для дискуссий, он ставит своей целью практическое воплощение принятых решений. Слушая сегодняшнюю дискуссию, я рад слышать конкретные предложения, созвучные тем сюжетам, которые стали предметом обсуждения на Всемирном саммите. Глобальная программа в области кибербезопасности (ГПК) предлагает рамочную основу, однако много времени и сил уделяется текущей работе с различными странами, чтобы обеспечить глобальное реагирование на национальные, региональные и глобальные киберугрозы и чтобы ни один человек не боялся выйти в интернет со своего мобильного телефона или компьютера. Одним особо важным направлением в этой широкой рамочной нише является Международное многостороннее партнерство против киберугроз (ИМПАКТ). Более 140 стран уже присоединились к этой глобальной инициативе, а некоторые государства получают от МСЭ помощь в создании на национальном уровне групп и центров реагирования на компьютерные инциденты. Иногда такие центры приходится создавать с нуля, и мы рады, что так много стран готовы поставить этот вопрос во главе повестки дня. Я думаю, наступил момент объединить наши усилия и обсудить сотрудничество в рамках ГПК на всех уровнях — как на высшем официальном, так и на оперативном. Это позволит обеспечить эффективность глобального реагирования на вызовы безопасности киберпространства.

МУЛЬТИСТЕЙКХОЛДЕРСКАЯ МОДЕЛЬ В УПРАВЛЕНИИ ИНТЕРНЕТОМ

ЯКУШЕВ: Наиболее важным вопросом, который освещается в окончательном докладе Рабочей группы по управлению интернетом, является необходимость укоренения подхода, уже упомянутого мной в связи с решениями Совета Европы. Речь идет о необходимости привлекать и обеспечивать равное участие всех основных групп заинтересованных участников, или, используя прижившийся англицизм, *стейкхолдеров* [stakeholders]. Значение термина *stakeholder* очень трудно без искажения смысла перевести на русский. Наиболее устоявшийся вариант перевода — «*заинтересованные участники».* В исходном, классическом варианте концепция мультистейкхолдеризма предполагала включение в процесс управления интернетом трех групп заинтересованных участников: правительств, частного сектора и гражданского общества. По мере того как концепция развивается, углубляется и наполняется практическим содержанием, к ним добавляются и другие сообщества. В итоге на сегодняшний день насчитывается уже пять категорий таких заинтересованных участников, или стейкхолдеров:

- правительства;
- частный сектор;
- гражданское общество;
- техническое сообщество;
- сами пользователи интернета как отдельное сообщество.

Неизменным остается то, что все участники должны сыграть одинаково важную роль. Это фундаментальный принцип, который должен учитываться при обсуждении будущего развития регулирования и управления интернетом, поскольку особая природа глобальной сети уже сейчас объединяет миллионы и миллиарды пользователей. Нам нужно использовать знания, опыт и возможности не только суверенных государств, но и частного сектора, компаний, которые разрабатывают технические стандарты интернета, и гражданского общества, заинтересованного в целом ряде вопросов, включая права человека, права потребителей и т.д. На сегодняшний день уже сложилась достаточно разветвленная система организаций, участвующих в управлении интернетом на международной уровне. Их список включает среди прочих Международный союз электросвязи (МСЭ) и ICANN. Что касается последней, то вряд ли ее можно охарактеризовать как международную или общественную организацию. Это некоммерческая корпорация со штаб-квартирой в Калифорнии, однако ее деятельность имеет глобальный масштаб. Именно ICANN вводит в эксплуатацию новые домены верхнего уровня и регулирует критически важные аспекты управления интернетом.

Существует ряд общих проблем, которые требуют совместного решения и сотрудничества. Во-первых, участие всех стейкхолдеров незаменимо во всех аспектах разработки и внедрения правовых норм в области управления интернетом и информационной безопасности. Мы наблюдаем аналогичную ситуацию в области освоения космоса, а возможно, даже в участии частных компаний в развитии атомной энергетики и эксплуатации источников атомной энергии. Поэтому участие всех заинтересованных сторон в управлении интернетом является обязательным условием дальнейшего успешного развития глобальной сети.

МАРКУС КУММЕР (**INTERNET SOCIETY**): Мне было очень приятно и интересно увидеть такой выраженный акцент на сотрудничестве с участием всех стейкхолдеров — мы в Обществе Интернета уверены в необходимости и правильности именно такого подхода. Однако я бы хотел сделать одну поправку или дополнение: в ходе нашей дискуссии зачастую звучит тезис о трех группах стейкхолдеров, однако на Всемирном саммите информационного общества в Тунисе мы добавили четвертую группу — представителей академического и технического сообществ. ISOC считает себя частью академического и технического сообщества и ассоциирует себя именно с этой группой заинтересованных участников процесса глобального управления интернетом. Кроме того, как уже ранее справедливо отметил М. В. Якушев, сегодня выделяется и пятая группа стейкхолдеров — непосредственно сообщество интернет-пользователей, чьи интересы также нельзя не учитывать.

БЕН БЕЙСЛИ-УОКЕР (ИНСТИТУТ ООН ПО ИССЛЕДОВАНИЮ ПРОБЛЕМ РАЗОРУЖЕНИЯ): Я бы хотел прокомментировать несколько моментов, так или иначе затронутых коллегами. Мне очень нравится идея участия в управлении глобальной сетью всего сообщества стейкхолдеров. Мои коллеги считают полезными мероприятия, на которых происходит обсуждение глобальной роли киберпространства и ведется поиск решений того, как мы собираемся этим пространством управлять и как мы будем формулировать политику в отношении интернета на национальном и международном уровнях. Однако мне кажется, что когда представители бизнеса, академического сообщества, а также лица, ответственные за выработку политического курса и принятие решений, собираются в одной аудитории, в 99 % случаев любое мероприятие распадается на три весьма интересные и насыщенные, но отдельные и невзаимосвязанные дискуссии. Между этими группами стейкхолдеров крайне редко наблюдается действительно эффективный диалог, особенно когда речь идет о тех пластах проблематики, с которыми работаю я в рамках Института ООН по исследованию проблем разоружения (ЮНИДИР), а также г-н Васильев в рамках своего ведомства, то есть

о роли киберпространства в контексте международной безопасности и глобальной политической динамики в этой сфере.

Мне также кажется, что международное сообщество профессионалов, занимающихся вопросами безопасности, особенно на дипломатическом уровне, не привыкло работать с неправительственным сектором и с бизнесом. Когда речь идет о ядерном оружии, нет такой острой потребности в участии негосударственных игроков в процессе переговоров и установлении нового режима, однако ситуация абсолютно противоположна, когда речь заходит о вопросах МИБ и глобального управления Сетью. Важно подчеркнуть, какая значительная часть интернета и его технической инфраструктуры сосредоточена в частных руках. У нас нет реально действующих механизмов, которые бы позволили нам пригласить людей, выросших в Силиконовой долине и привыкших крайне подозрительно относиться к правительству, на встречу с дипломатами и сказать им: давайте все вместе подумаем, как нам решить проблему. Этот момент следует учитывать и понимать его возможные последствия.

ВЕБЕР: Я бы хотел еще раз вернуться к идее участия всего сообщества стейкхолдеров в управлении интернетом. Мне кажется, эта идея совсем не означает, что можно обойтись вообще безо всякой рамочной правовой основы. Нам необходима система, которая в правовом плане является стабильной и устойчивой — я сейчас пользуюсь терминами, которыми обычно оперируют технические специалисты. Скорее всего, единственным источником, к которому мы можем обратиться за какими-то правовыми принципами, является международное *обычное* право. В этой области у нас также есть некоторые принципы, сформулированные Обществом Интернета (ISOC) и общепринятые в широком правовом сообществе.

М. В. Якушев в своей реплике упомянул договор о космосе. Это многосторонний документ, однако содержащиеся в нем ключевые принципы могут с успехом применяться и в других сферах. К примеру, у нас есть определенные законы, которые регулируют международное судоходство. Существуют и действуют законы о реках. В течение уже более 100 лет общепринято, что сторона, находящаяся у истока реки, не имеет права сбрасывать в нее опасные химикаты, поскольку это нанесет ущерб стороне, расположенной ниже по течению. Так что, скорее всего, при разработке будущих законопроектов в области национальной безопасности нам придется анализировать существующие принципы международного права, включая международное обычное право, чтобы понять, какие принципы являются общепринятыми.

В международном праве присутствует более или менее общепринятый принцип о недопущении трансграничного ущерба — превентивный принцип, зафиксированный в Декларации по окружающей среде и развитию, принятой в Рио-де-Жанейро в 1992 г., а также в некоторых документах Совета Европы и других международных организаций. Отталкиваясь от подобных принципов, мы могли бы попытаться положить начало дальнейшему обсуждению, которое неизбежно должно затронуть следующие вопросы: какие принципы могут получить дальнейшее развитие и что из них могло бы стать частью какого-то нового международного документа? Скорее всего, речь не будет идти о новом юридически обязывающем международном договоре: я не очень верю, что правительствам стран по всему миру удастся достичь согласия относительно такого документа. Но можно подумать о новых инструментах мягкого права, таких, например, как кодифицированные принципы и правила поведения.

УОЛТЕР РИД (ПОСТОЯННОЕ ПРЕДСТАВИТЕЛЬСТВО США НА КОНФЕРЕНЦИИ ПО РАЗОРУЖЕНИЮ В ЖЕНЕВЕ): В ходе обсуждений и переговоров о мерах по укреплению доверия с Россией и некоторыми другими государствами — вне зависимости от того, было ли у нас абсолютно согласованное правовое определе-

ние этого термина — часто обнаруживалось, что никакого готового определения вообще не существует. Меры, которые мы можем предпринять в сфере безопасности киберпространства, часто возможны только благодаря партнерству между государственными и негосударственными игроками. Г-н Якушев с этим, очевидно, тоже столкнулся. В США ситуация в области регулирования киберпространства именно такова: очень многие меры невозможны без сотрудничества с частным сектором, с негосударственными стейкхолдерами, которые привлекаются на основе добровольного сотрудничества. Поиск решений существующих проблем требует именно такого типа сотрудничества. Я думаю, такая ситуация станет нормой в течение следующих 10–15, максимум 20 лет, и именно в направлении развития модели мультистейкхолдеризма будет вестись основная работа. Учитывая абсолютную необходимость участия множества стейкхолдеров — это вполне здоровая ситуация, и очень хорошо, что правительства регулярно получают об этом напоминания. Так что мы считаем очень важным обсуждение этих вопросов на международном уровне, особенно в контексте проблем международной безопасности. Я благодарен ПИР-Центру за то, что он выводит эту дискуссию на уровень российско-американского гражданского сообщества, и считаю это очень важным шагом.

ОРЛОВ: Большое спасибо, г-н Рид. Пару недель назад к нам в Москву приезжала заместитель государственного секретаря США Роуз Готтемюллер. Конечно, к ней выстроилась очередь, чтобы поговорить об Иране или проблемах противоракетной обороны (ПРО), однако она начала разговор с вопроса о том, как информационные технологии могут изменить мир в сфере контроля над вооружениями и во многих других сферах. У нас состоялось оживленная и продуктивная беседа, которая продемонстрировала, что мышление в американской администрации действительно вышло на весьма высокий уровень, и это нас очень вдохновляет.

РИД: Тем, кто работает здесь, в Швейцарии, наверное, известно о проекте MELANI (Центр сбора и анализа информации). Это программа партнерства между государством и частным сектором, причем в данном случае речь идет о партнерстве между полицией и частным бизнес-сообществом. Это партнерский проект, который создает безопасное пространство между полицейским сообществом и теми сегментами бизнес-сообщества, наиболее подверженными киберпреступности и незаконным действиям в киберпространстве. Данный проект, скорее всего, не поможет исправить уже случившееся — я имею в виду ущерб, понесенный бизнесом от уже совершенных актов киберпреступности, но он поможет лучше понять, что происходит и как себя защитить в дальнейшем, поможет стать частью широкого сообщества пользователей. В проекте сочетаются элементы как государственного, так и частного участия, так что речь не идет об официальном государственном проекте. Деятельность MELANI помогает интернет-пользователям предотвратить повторение подобных ситуаций в будущем, и эта работа ведется на уровне провинций, а также на уровне муниципалитетов во многих странах по всему миру. Что-то подобное появляется в США, в Канаде — обычно на муниципальном, субнациональном уровне. В Швейцарии этот проект пока имеет экспериментальный статус, но такой пример может быть полезен и другим государствам, в том числе России.

РОССИЯ И ЕЕ МЕСТО В РЕГУЛИРОВАНИИ МИБ И УПРАВЛЕНИИ ИНТЕРНЕТОМ

ЯКУШЕВ: Хотелось бы сказать несколько слов о позиции России в области глобального регулирования информационного пространства и обеспечения МИБ, о том, какие предложения выдвигаются российской стороной и какие есть воз-

можности для сотрудничества, а также сделать некоторые выводы, которые можно будет обсудить в ходе нашей дискуссии.

К сожалению, у моей страны, как это принято считать, в основном за рубежом, — *плохая кредитная история*. Речь идет о распространенном мнении, что с учетом якобы практикуемой цензуры и политических ограничений на свободу общения в интернете Россия находится не в том положении, чтобы вносить какие-либо предложения в международную повестку или проявлять какую-то активность в сфере МИБ и управления интернетом. Кибератаки против Эстонии, Грузии, оппозиционных российских вебсайтов спровоцировали множество вопросов, причем многие из них действительно до сих пор остаются без ответа.

Однако, будучи не российским официальным лицом, а независимым исследователем и экспертом, я могу сказать, что все подобные мнения и слухи не имеют ничего общего с реальностью. На самом деле в России на данный момент существует свободная система и достаточно либеральная модель регулирования интернета, особенно по сравнению с Казахстаном, Китаем, Ираном или Туркменией. В частности, отсутствуют какие-либо серьезные ограничения на поток информации в Сети, нет цензуры в отношении интернет-транзакций, что, конечно, отличается от ситуации с телевидением или радиовещанием. В России интернет действительно остается зоной свободных коммуникаций. В этом плане Россия имеет очень хорошую *кредитную историю*, что весьма актуально, когда речь заходит об информационной безопасности и управлении интернетом. Более того, политические заявления российского руководства до последнего времени демонстрировали готовность правительства не вводить никаких ограничений на свободу в интернете. Это хорошо, поскольку определенные идеи насчет введения подобных ограничений все же обсуждались и продолжают обсуждаться на высоком политическом уровне.

Однако российское правительство внесло определенные предложения, которые не находят единогласной поддержки на международном уровне. В частности, речь идет о концепции Конвенции об обеспечении международной информационной безопасности и предлагаемых *Правилах поведения в области обеспечения МИБ,* проект которых был направлен генсеку ООН четырьмя государствами — членами Шанхайской организации сотрудничества (ШОС) при ведущей роли России. Иногда эти инициативы воспринимают как российскую реакцию на американские концепции и стратегические документы, опубликованные чуть раньше, в прошлом 2011 г. Но если изучить и проанализировать *концепцию Конвенции об обеспечении МИБ*, становится ясно, что в этих предложениях нет ничего особо опасного, странного или неприемлемого для международного сообщества. Концепция Конвенции содержит ряд весьма востребованный сегодня определений: что такое кибервойна, или, точнее говоря, что такое информационная война, что такое информационное оружие, информационные системы, пусть эти определения в текущей редакции и не бесспорны.

В России избегают использования приставки *кибер-*, вместо нее предпочитают использовать прилагательное *информационный*. Концепция Конвенции перечисляет многие угрозы миру и международной безопасности, в том числе деструктивные действия в информационном пространстве, диверсионные действия, психологические войны, информационную экспансию. Возможно, иногда это действительно напоминает риторику холодной войны, когда у нас часто велась речь об *идеологической войне* американцев против Советского Союза. Сейчас существуют некоторые отличия, но эта угроза входит в список основных угроз, выделяемых авторами документа. В этой связи нельзя забывать о существовании принципов международного информационного права. Основным принципом является суверенитет государства над национальной инфраструктурой. На практике этот принцип означает, что все, что технически и физически расположено в пределах российских границ, должно регулироваться российскими законами.

Именно так Россия и некоторые другие страны хотят воплощать в жизнь принцип своего суверенитета над собственным киберпространством — или информационным пространством. В инициативах России и стран ШОС также прописаны меры по предотвращению военных конфликтов, информационных войн, меры по борьбе с терроризмом в киберпространстве, меры по борьбе с киберпреступностью, в том числе уголовные и другие правовые меры.

К сожалению, эти предложения были встречены многими государствами и экспертными сообществами весьма прохладно. Каковы причины столь негативного отношения? Причиной *номер один* является то, что при подготовке и инициировании этих предложений не применялся принцип участия всех заинтересованных сторон. Не применялся он и при обсуждении этих предложений на международном уровне. Российское интернет-сообщество не было приглашено к участию в разработке этих предложений, и поэтому в них присутствуют определенные ошибки, пробелы, а местами, может быть, и недостаточно хорошо проработанные, с юридической точки зрения, формулировки. Естественно, это не позволяет представителям российского экспертного сообщества безоговорочно поддержать подобные идеи. Но я бы хотел еще раз подчеркнуть, что фундаментальных изъянов в российских предложениях нет.

Что же касается суверенитета России над технической инфраструктурой в российском информационном пространстве, то здесь требуются дальнейшие теоретические исследования, чтобы понять, должен ли такой суверенитет быть абсолютным. К примеру, Олимпийские игры — это полностью неправительственное мероприятие, которое вносит многомиллиардный финансовый вклад в экономику многих стран, которые их принимают, организуют и участвуют в них. Но если Олимпийские игры проводятся в такой стране, как Россия, то есть игры в Сочи в 2014 г., то для их обеспечения будет использоваться инфраструктура и техническое оборудование, находящиеся в России. Несмотря на это, правила игр не могут определяться российским ФСБ или даже российским правительством — они определяются Международным олимпийским комитетом (МОК). При этом все страны, в том числе Россия, признают, что некоторые виды деятельности регулируются правилами, которые не могут определяться национальным законодательством, иначе они становятся невозможными.

Естественно, такие предложения требуют обсуждения, и необходимо еще более детально обсудить российские предложения в области МИБ. Возможно, нам следует обсуждать их в свете американских концепций и предложений, изложенных в национальной стратегии по действиям в киберпространстве американского Белого дома от 2011 г. Но есть еще один важный вопрос: следует ли нынешние (либо возможные будущие) российские предложения рассматривать как альтернативу или замену Будапештской конвенции *О киберпреступности*, которую Россия не подписала и не ратифицировала? Как уживутся эти документы? Будут ли они конкурировать или взаимно дополнять друг друга? Это открытый вопрос, требующий не менее пристального внимания.

ОРЛОВ: В докладе М. В. Якушева была затронута тема баланса между правительственными и неправительственными дискуссиями в России касательно роли интернета, будущего *Рунета* и информационной безопасности. Есть некоторые замечательные российские авторы, которые предполагают, что через 20–30 лет в России уже не останется *сети интер-нет*, а вместо нее будет лишь *сеть интерда*, которая будет автоматически одобрять все правительственные решения. Один из этих авторов — Владимир Сорокин, который отлично пишет на эту тему. Но судя по тому, что мы сейчас видим и слышим, такие пессимистические прогнозы, конечно, кажутся неоправданными. Я бы даже сказал, что российские власти и российские госструктуры сейчас довольно внимательно прислушиваются

к взглядам сообщества российских неправительственных организаций, особенно тех организаций, которые действительно разбираются в своих вопросах.

М. В. Якушев скромно не упомянул о своем участии в четырехчасовой встрече представителей российского интернет-сообщества с Д. А. Медведевым в 2011 г., когда тот занимал должность президента России. Мне было очень интересно читать протокол той встречи: президент часто использовал английские слова, потому что трудно было подобрать подходящие русские. В ходе встречи и общения президента с ее участниками также высветилось немало противоречий, которые я бы назвал *позитивными противоречиями*.

ВИКТОР ВАСИЛЬЕВ (ПОСТОЯННОЕ ПРЕДСТАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ ПРИ ООН И ДРУГИХ МЕЖДУНАРОДНЫХ ОРГАНИЗАЦИЯХ В ЖЕНЕВЕ): Не могу согласиться с некоторыми высказанными сегодня взглядами. Один из них — это представление о том, что Россия якобы имеет *плохую историю* в сфере информационной безопасности. Я бы сказал, что у Российской Федерации, напротив, вполне позитивная история в этой области. Именно наша страна первой из всех государств подняла вопрос информационной безопасности на международной арене — мы сделали это в 1998 г. на площадке ООН. С тех пор мы выступили соавторами всех резолюций Генеральной Ассамблеи ООН по вопросам информационной безопасности. Конечно, у нас проходят плодотворные дискуссии, и российские участники уже неоднократно высказывали свои взгляды на эти вопросы. Мы понимаем, что точки зрения по разным аспектам могут отличаться, поскольку обсуждается очень широкая и сложная проблематика. Конечно, есть вопрос свободы слова, свободы информации и другие связанные вопросы.

Российская позиция как раз и представляет попытку инициировать обсуждение комплекса проблем, составляющих *триаду* информационной безопасности. Несмотря на то что многие западные страны могут не разделять российские взгляды, отраженные в наших документах, то есть в концепции Конвенции об обеспечении МИБ и в проекте Правил поведения в области обеспечения МИБ. Поэтому сейчас Россия и ее партнеры закладывают фундамент для такого обсуждения, представляют российскую позицию по некоторым вопросам, и мы выступаем соучастниками этой дискуссии. Мы также выделяем финансирование Институту ООН по исследованию проблем разоружения, который в этом году проводит ряд мероприятий в этой сфере, а также оказывает экспертную поддержку Группе правительственных экспертов (ГПЭ ООН) по МИБ. Группа представит свои взгляды на сессии Генеральной Ассамблеи ООН по вопросам информационной безопасности, запланированной на 2013 г.

Я считаю, что основной задачей для нас и наших партнеров является поиск точек соприкосновения по данным проблемам. Конечно, по некоторым вопросам у нас будут разногласия ввиду разных правовых подходов, различной доктринальной логики и т.д. Но есть и вопросы, по которым мы единодушны: это вопросы терроризма, преступной деятельности в интернете, проблемы мошенничества с кредитными картами, детская порнография и т. п. Нужно определить те сферы, где мы можем сотрудничать на международном уровне, где мы можем ввести нормы, которые помогут предотвратить подобные нарушения и которые будут способствовать успеху дискуссии на международном уровне по широкому кругу вопросов, в том числе по вопросу *красной кнопки* и т.д. Для этого нам нужна площадка для обсуждения, нам необходим форум. Нужно также решить, какие из существующих площадок лучше всего подходят для этих целей, имея в виду прежде всего ООН, МСЭ, Всемирную организацию интеллектуальной собственности (ВОИС) и ЮНИДИР, в рамках которых ведется обсуждение различных элементов информационной безопасности. Так что давайте над этим работать, давайте обдумывать эти вопросы и решать, в каких областях мы можем сотрудничать на практическом уровне.

БЕЙСЛИ-УОКЕР: Как только что отметил г-н Васильев, в российской концепции Конвенции об обеспечении информационной безопасности нет фундаментальных изъянов. Я не хотел бы сейчас давать оценки российскому предложению, но у меня нет сомнений, что между позициями американского и российского правительства существуют огромные различия на самом фундаментальном концептуальном уровне. Если попытаться более детально вникнуть в этот сюжет, становится очевидно, что мы имеем дело с двумя фундаментально разными по своей природе ответами на вопрос о том, является ли информация сама по себе оружием или нет. Возвращаясь к точке зрения В. Л. Васильева, я бы предположил, что в сегодняшних условиях международному сообществу будет крайне трудно достичь согласия, если не снять с повестки дня такие вещи, как российский проект глобального и юридически обязывающего документа ООН в области регулирования киберпространства. Есть много конкретных областей, по которым действительно можно достичь согласие, и мы не должны позволить определенным глобальным политическим вопросам затмить целый ряд потенциальных практических решений в рамках *мягкого* права, мер по укреплению доверия или правил поведения.

РИД: Продолжая мысль г-на Бейсли-Уокера, с точки зрения США я бы упомянул следующие моменты. Конечно же, перед нами стоит ряд вопросов в области безопасности, ряд вопросов в области киберпространства (как уже было отмечено, мы используем разные термины: с одной стороны, информационные и телекоммуникационные технологии, с другой — приставка *кибер*-). Но я полностью согласен с мыслью о том, что различия в терминологии или даже в концептуальном понимании не должны препятствовать нашему сотрудничеству. Мы рады тому, что эта беседа состоялась, мы также рады, что Россия еще в 1998 г. поставила на повестку дня ООН вопрос о глобальном регулировании информационной безопасности в рамках Объединенных Наций. Мы с большой готовностью подключились к этому процессу. Эти вопросы приобретают все большую важность в российско-американских двусторонних отношениях. Они получили развитие в виде обсуждения мер по укреплению доверия в наших двусторонних отношениях. Мне кажется, направленность американского взаимодействия с Москвой в данной области должна и впредь состоять в том, чтобы не позволить терминологическим противоречиям и дискуссиям, которые могут тянуться десятилетиями, помешать нам понять друг друга на практическом уровне, поддерживать контакты и сотрудничать во многих конкретных областях, где у нас есть общие цели. Поэтому мне кажется, что нужно идти путем мер по укреплению доверия, и здесь мы рассчитываем на межправительственную поддержку. Именно здесь мне видится весьма многообещающий потенциал для сотрудничества.

КИБЕРУГРОЗЫ И КИБЕРВЫЗОВЫ

ЯКУШЕВ: Международные форумы по вопросам управления интернетом проводятся ежегодно. Существует сеть региональных, местных и национальных форумов по управлению интернетом, которые проводятся в разных странах, в том числе и в России. Давайте сконцентрируемся на таком конкретном аспекте глобального управления интернетом, как *интернет-безопасность*. Существуют три или четыре уровня, которые требуют разных методов регулирования и которые имеют различные последствия в плане глобальной информационной безопасности.

- Проблема предотвращения *кибервойн* относится к уровню международных и межправительственных отношений, уровень международного права.
- *Кибертерроризм* и предотвращение атак, имеющих в своей основе политическую мотивацию и направленных против правительств, государственных органов и общества в целом.

- *Киберпреступность* — преступления, совершаемые обычными гражданами и пользователями интернета, в том числе такие незаконные действия, как мошенничество, кража личных данных и т.д. К сожалению, такие преступления в настоящее время широко распространены, более того, глобальный и национальные рынки киберпреступности активно развиваются и растут.

За последние пять лет в глобальной сети были отмечены определенные тенденции, связанные с развитием этой *триады угроз*. Мы видим необходимость в принятии мер, направленных против незаконного использования интернета и на недопущение его использования с целью подрыва международной безопасности. В основном об этом принято говорить в связи с такими инцидентами, как кибератаки в Эстонии, которые произошли пять лет назад (в 2007 г.) и были направлены против важных ресурсов и объектов инфраструктуры, которым в течение длительного времени был нанесен существенный ущерб. Тогда в самой Эстонии и на международной арене присутствовало понимание того, что источник атак находится за пределами страны и что они представляют определенную форму внешнего вмешательства. Эстонцы подозревали, что все эти атаки были организованы российским правительством, которое, естественно, опровергало обвинения, не имеющие под собой твердых доказательств.

БЕЙСЛИ-УОКЕР: Я согласен с классификацией, которая разделяет угрозы безопасности киберпространства на кибервойны, кибертерроризм и киберпреступность. Но мне кажется, что в процессе нашего сегодняшнего обсуждения также высвечивается смешение этих категорий. Очень легко говорить о четких классификациях, но как только мы начинаем обсуждать их предметно, границы между ними начинают размываться. Конечно, это представляет собой проблему для международного сообщества — проблему проведения четких терминологических, концептуальных и, впоследствии, нормативных границ. Как это сказывается на попытках эффективного регулирования и эффективного дипломатического взаимодействия в сфере безопасности киберпространства? Как провести черту между организуемой и направляемой государством кибератакой и кибертерроризмом, то есть в тех случаях, когда неизбежно приходится принимать во внимание правовые режимы? Где проходит эта черта? На все эти вопросы до сих пор нет четких ответов.

ВЕБЕР: Мне кажется, нам нужно обсуждать общие темы, которые представляют интерес для многих стран, чтобы получить некий общий ответ. Сложность, конечно, состоит в том, что все говорят о необходимости борьбы с кибертерроризмом. Невозможно найти человека, который скажет, «да, кибертерроризм — это полезная вещь». Проблемы начинаются, как только задается вопрос, а что такое кибертерроризм и кто такие кибертеррористы? В разных странах определение терроризма очень сильно отличается, не говоря уже об отсутствии согласованного определения кибертерроризма, то есть концептуальные и терминологические трудности возникают в самом начале обсуждения.

ОРЛОВ: Позвольте мне привлечь внимание к Олимпийским играм 2014 г. в Сочи в контексте информационной безопасности. Этот вопрос находится в первых строках повестки дня новоизбранного президента Путина; он также очень интересует некоторые швейцарские компании, которые плотно участвуют в подготовке к играм. Несмотря на нерешенный вопрос о том, имеем ли мы дело с неправительственной, межправительственной или другой деятельностью, факт остается фактом — война вокруг Олимпийских игр уже началась. Официальный российский вебсайт игр уже подвергся атаке в 2011 г., его работа была парализована на несколько дней. Этот эпизод стал явным сигналом того, что с приближением игр кибервойна вокруг них станет еще более ожесточенной.

Я бы хотел высказать некоторые соображения нашим швейцарским коллегам, которые так успешно выступают в роли посредников между Россией и Грузией.

В киберпространстве выступать в роли посредника очень нелегко. Как предотвратить DDoS-атаки? Кто является владельцем защитных систем — волшебных стен, которые выступят преградой на пути таких атак? Я выяснил, что сегодня в этой роли в качестве действительно серьезного игрока выступает всего лишь одна компания — американская компания, которая тесно связана с Министерством обороны США. Только у нее на самом деле есть эффективное решение против массированных DDoS-атак. Однако я надеюсь, что в России тоже будет достигнут прогресс в вопросах предотвращения таких видов кибератак.

Также заслуживает внимания корреляция между кибербезопасностью и другими видами угроз безопасности. Я имею в виду ядерную безопасность и атаки, направленные против ядерной инфраструктуры Ирана, которые оказались очень результативными. Эти атаки напугали иранцев, а израильтяне гордятся результатами атаки с использованием вируса *Stuxnet*. После этого по всему миру эхом прокатилась серия проблем, начиная от иранской ядерной инфраструктуры и заканчивая российскими объектами, по крайней мере в плане риска пролиферации таких атак. Кроме того, ракетные объекты Ирана тоже столкнулись со значительной угрозой — не физически, а через киберпространство. Это лишь один пример, близкий к тематике моих исследований. Но для меня он стал демонстрацией серьезности такого сочетания кибервойн и ядерной безопасности.

ВЕБЕР: В борьбе с кибератаками вопрос состоит в том, можно ли получить доступ к лицу, которое отвечает за конкретный IP-адрес. По крайней мере, согласно швейцарскому законодательству, это очень непростая процедура, она становится возможна только в случае проведения уголовного расследования. Существуют решения Верховного суда и Апелляционного суда кантона Берн, согласно которым частные организации, собирающие данные об IP-адресах, фактически не имеют права раскрывать эти адреса по каким бы то ни было причинам другим частным организациям, поскольку это будет нарушением законодательства о защите данных. Данное ограничение может быть снято, если ведется уголовное расследование. Прокурор имеет право попытаться установить личность, скрывающуюся за IP-адресом. Но, откровенно говоря, очень трудно понять, кому в таких случаях направлять свою жалобу. Кантону Женева? Федеральному прокурору? Какому-либо прокурору? Даже если мы получим ответ на вопрос о том, в какие органы следует адресовать тот или иной запрос, сразу возникает следующий вопрос: действительно ли в таких случаях применимо именно швейцарское законодательство? Трудно сказать. Возможно, применять следует законы не Швейцарии, а той страны, гражданином которой является конкретное лицо?

Таких вопросов очень много, и найти на них ответы нелегко. В области международного уголовного законодательства у нас также нет юридически обязывающих международных договоров, за исключением Конвенции Совета Европы *О киберпреступности*, которая действует на территории не только Центральной Европы, но и Восточной Европы, Средней Азии и даже в некоторых странах за пределами нашего континента. Однако, повторюсь, пока что у нас в этой области имеется больше проблем, чем решений.

НАДЕЖДА СИКОРСКАЯ (**NASHA GAZETA.CH**): Я — редактор русскоязычной швейцарской газеты, и у меня есть вопрос к участникам нашей дискуссии. Сайт *Нашей Газеты* в феврале 2012 г. подвергся нападению — DDoS-атаке с использованием ботнета — и едва не был полностью уничтожен, причем по непонятным нам причинам. С точки зрения содержания сайта, единственная возможная причина, которая приходит мне в голову, — это опубликованная статья на тему Олимпийских игр в Сочи, которая носила довольно критический характер. Кроме того, нападение произошло за несколько недель до президентских выборов в России, хотя по вопросу выборов мы не занимали какой-либо конкретной позиции. Тем не менее на нас напали, и на восстановление работы ресурса ушло довольно мно-

го времени, причем работа сайта восстановилась с большими трудностями. Наше расследование показало, что в качестве промежуточного звена при атаке были задействованы серверы, находящиеся на территории России и Китая. В то же время понятно, что такая информация не указывает на определение изначального источника атаки, поскольку можно использовать серверы-зеркала и другие технологии. Сайт нашей организации является русскоязычным, зарегистрирован в Швейцарии и размещен в домене *.ch*. Есть ли какая-то инстанция, куда мы можем направить жалобу? Кто занимается расследованием таких случаев и что мы можем сделать как пользователи и как жертвы нападения?

ЯКУШЕВ: Что касается незаконного использования интернет-технологий и технологий мобильной связи, то мы живем в мире, который с каждым днем становится все сложнее. Если вспомнить историю, поначалу даже практическое применение электричества или импорт картошки и помидоров из Америки в Европу создавали серьезные проблемы. Люди ели несъедобные части привозимых растений, например, ядовитые листья и цветки. Электричество также представляло опасность при неправильном обращении, не говоря уже об атомной энергии и более сложных технологиях. Аналогичным образом, у интернета есть как преимущества, так и недостатки, и нам нужно понять как сделать нынешний мир с его новыми технологиями безопаснее. К примеру, когда в 2011 г. в Лондоне прошли уличные беспорядки, резкой критике подверглось заявление британских властей о том, что они могут ввести определенные ограничения на доступ в интернет с коммуникаторов *Blackberry*. Всем было очевидно, что проблема заключалась не в интернете или интернет-технологиях, а в социальных проблемах в Великобритании. У нас нет *красной кнопки*, и мы не можем, к примеру, просто взять и навсегда отключить технологии *Blackberry* или интернет-соединение в масштабах страны.

Что же мы можем сделать? В первую очередь внедрить более совершенную систему идентификации граждан, которые используют определенные технологии коммуникации, мобильные телефоны и IP-адреса, доменные имена, и вести работу в этой области совместно с Обществом Интернета (ISOC). Я думаю, что российские и иностранные неправительственные организации, российское правительство и российские правоохранительные органы должны работать сообща, чтобы добиться осязаемых и положительных результатов, ничего при этом не запрещая неизбирательно и делая использование новых технологий безопаснее.

ПРОБЛЕМА *КРАСНОЙ КНОПКИ* — ОТКЛЮЧЕНИЕ ИНТЕРНЕТА

ЯКУШЕВ: В ходе нашей дискуссии мы также не можем не принимать во внимание пример *Арабской весны*, когда социальные сети сыграли определенную роль в ее событиях, помогли вывести людей на улицы и организовать акции, которые в итоге закончились сменой политического режима в данных странах и социально-политическими переменами. Пример Египта весной 2011 г. вновь продемонстрировал так называемую проблему *красной кнопки,* то есть масштабного целенаправленного отключения интернета на территории суверенного государства.

Египетский прецедент ставит нас перед массой вопросов, которых мы сегодня еще не касались. Можно ли отключить интернет на глобальном уровне или, возможно, существуют варианты его пошагового отключения на национальном уровне? Могут ли в киберпространстве применяться принципы, определяющие фундаментальные права человека? Какие виды деятельности нельзя допускать в Сети? Как выработать необходимые правила, которые учитывают основные права и свободы человека — к примеру, свободу слова, свободу распространения информации, свободу доступа к информации и доступа к интернету? Все эти вопросы однозначно должны быть вынесены на обсуждение.

ВАСИЛЬЕВ: Вопрос, который М. В. Якушев назвал проблемой *красной кнопки*, состоит прежде всего в том, кто контролирует *красную кнопку* и при каких обстоятельствах она может быть нажата. Каков политический и правовой порог для использования *красной кнопки* с целью отключения интернета? События *Арабской весны* невольно заставляют задуматься о любопытной тенденции. Если в содержании сетевых протестов присутствуют политические лозунги, такие как призывы к независимости и свободе, которые апеллируют к правам человека и так далее, нажимать *красную кнопку* нельзя. Получается, использовать ее можно только против хулиганов, координирующих свои действия в Сети, что обсуждалось властями Великобритании во время лондонских беспорядков 2011 г.? Это еще одна тема для широкой дискуссии.

Далее, профессор Вебер затронул вопрос выхода в интернет через мобильные телефоны. Дело в том, что во многих странах нет объективной необходимости контролировать связь между мобильными телефонами и провайдерами вебсайтов. Но давайте возьмем, к примеру, Россию, где теракты на Северном Кавказе происходят с достаточно высокой интенсивностью. Наглядный пример: когда произошли взрывы в московском метро в 2011 г., нашим службам безопасности пришлось отключить доступ в интернет с мобильных устройств, чтобы предотвратить дальнейшие взрывы. Такое решение было принято с учетом того, что некоторые из использованных взрывных устройств управлялись и приводились в действие при помощи мобильных телефонов. Очевидно, что в таких случаях ограничение мобильной коммуникации необходимо и действия спецслужб не следует рассматривать в качестве негативного примера использования *красной кнопки*.

ВЕБЕР: У меня есть короткий комментарий к очень интересной мысли, которую высказал г-н заместитель посла. Насколько я помню, я ни разу не упоминал прямые сравнения между разными странами, потому что хорошо понимаю: экспертам не следует *показывать пальцем* на те или иные страны. Тем не менее, поскольку я занимаюсь преподавательской деятельностью в Восточной Азии, хотелось бы привлечь ваше внимание к ситуации с *красной кнопкой* в этом регионе. Считается, что среди восточноазиатских государств нажать *красную кнопку* чаще всего пытается Китай. Однако, с другой стороны, *красную кнопку* также довольно часто нажимает Сингапур, который, как мы знаем, коммунистической страной не является. Так что нам нужно быть очень осторожными, когда речь заходит о сравнительных оценках государств в части свободы интернета. Технологически легче отключить мобильные телефоны, чем традиционные компьютерные сети — по крайней мере, если компании заинтересованы в сотрудничестве с правительством. Именно так и было в случае с Египтом в 2011 г., где интернет отключили, поскольку в определенный момент об этом настойчиво попросило правительство.

ЯКУШЕВ: Что касается самого понятия *красной кнопки*, то это, конечно, фикция. В прошлом сентябре я был в штаб-квартире ICANN и постарался обойти там все кабинеты — никакой *красной кнопки* я не нашел. Кое-кто утверждает, что *кнопка* находится в вашингтонском офисе, так что, может быть, я просто проверял не в том месте, ведь я был в Калифорнии. Что же касается *красной кнопки* в России, то я искренне горжусь тем, что живу в стране, где подобные технологии и методы никогда не использовались — и с этой точки зрения в нашей стране действительно отсутствует цензура в интернете. Мы должны этим гордиться.

КУММЕР: У нас состоялась интересная дискуссия по поводу *красной кнопки*, и я думаю, что г-н Вебер и г-н Васильев уже дали ответ на этот вопрос. Иногда эту кнопку также называют *рубильником смерти [killer switch]*. Технические эксперты использовали этот термин, когда обсуждался вопрос о том, как удалось так быстро отключить интернет в Египте во время событий *Арабской весны*. По существу, ответ заключается в том, что архитектура глобальной сети в республике была очень несовершенна: чрезмерно централизована. Если архитектура интернета

спроектирована должным образом, то это очень распределенная и очень устойчивая система. Ведь в свое время именно такая задача была поставлена перед теми, кто стоял у истоков интернета: создать сеть, которая сможет выдержать даже массированный ядерный удар. Во время природных бедствий, таких как цунами в Японии в 2011 г. или землетрясение на Гаити в 2010 г., интернет оказался едва ли не единственным работающим средством связи. Вся остальная инфраструктура, за исключением спутниковой связи, вышла из строя, а интернет продолжал функционировать, и люди могли связаться друг с другом через Сеть. Поэтому если архитектура интернета спроектирована и сбалансирована должным образом, то никакого *рубильника смерти* в Сети не существует.

Что же касается международного сотрудничества, то оно просто незаменимо. Мы должны сотрудничать и мы должны вести обсуждения. Рассматриваемая нами проблема имеет много общего с терроризмом: общепринятого определения того, что такое терроризм, на международном уровне до сих пор не существует. То же самое можно сказать о детской порнографии и массе других проблем, связанных с безопасностью киберпространства. Общепринятых и универсальных определений этих проблем у нас пока нет. Ключевой международной площадкой для обсуждения проблем и определений является Форум по управлению интернетом, который работает под эгидой ООН, созывается от имени генерального секретаря ООН и в котором участвует множество стейкхолдеров. При поиске решений необходимо прислушиваться ко мнению всех стейкхолдеров. Государство и правительство находится на острие решения проблем безопасности, однако очень важно, чтобы власти прислушивались к тому, что говорит гражданское общество, у которого обычно существуют серьезные озабоченности в сфере прав человека. Не менее важно также обсуждать с техническим экспертным сообществом вопрос о том, насколько осуществимы предлагаемые технологические меры решения. И, конечно же, все стейкхолдеры должны работать и действовать сообща.

ОРЛОВ: Большое спасибо! Я думаю, что нам уже удалось многого добиться во время сегодняшней встречи, особенно благодаря нашим докладчикам, основному докладчику и комментатору. Я очень ценю работу и усилия, предпринятые г-ном Якушевым и профессором Вебером, и я уверен, что нам еще есть много что сказать, так что наш разговор не ограничится сегодняшней встречей. Мы бы хотели объединить усилия и в ближайшие месяцы принять участие в дальнейшей широкой международной дискуссии по поводу принципиальных вопросов кибербезопасности и управления интернетом.

В 2013 г., на следующем ежегодном заседании с участием членов *Centre russe d'etudes politiques* и сообщества Международного клуба *Триалог* мы планируем обсудить довольно близкие темы, такие как новые угрозы безопасности, в том числе финансовые преступления и вопросы связи между отмыванием денег, терроризмом и финансированием программ по разработке оружия массового уничтожения. Однако тема, которую мы обсуждали сегодня, вне всяких сомнений, остается одним из основных направлений исследований, проводимых ПИР-Центром, в рамках которого активно развивается проект «Международная информационная безопасность и глобальное управление интернетом». Пока что проект базируется преимущественно в Москве, однако широкое и интенсивное сотрудничество с иностранными экспертами, аналитическими центрами и международными организациями станет важным шагом в дальнейшем развитии нашего проекта. Ряд проблем, которые мы сегодня затронули, требуют быстрого и хорошо продуманного вклада неправительственного сообщества, в том числе ПИР-Центра, в обеспечение процесса принятия политических решений в России соответствующей аналитической базой.

Национальная политика в области защиты критической инфраструктуры пока не приобрела в России системного характера. Еще только предстоит решить, какой

подход должен использоваться в данной сфере. Кроме того, по мере быстрого развития российского рынка киберпреступности нарастает обеспокоенность в связи со все более изощренными, многочисленными и масштабными преступными действиями как в национальных российских сетях, так и за их пределами. Здесь, как уже было отмечено докладчиками и комментаторами, Россия должна предложить собственный подход к развитию эффективного международного сотрудничества по борьбе с киберпреступностью, поскольку Будапештская конвенция, похоже, не рассматривается в качестве оптимальной основы для российского участия в подобных механизмах. Наконец, благодаря всем участникам сегодняшней встречи, мы получили весьма подробную и разноплановую картину стратегических дискуссий в области межправительственного регулирования вопросов информационной безопасности, включая предложения в этой сфере, внесенные Россией и государствами-членами ШОС.

Еще более важен тот факт, что мы, как это ни удивительно, пришли к очень четкому общему пониманию того, что нужно делать, для того чтобы стимулировать сотрудничество между Россией и ее западными партнерами, несмотря на то что пока между нами сохраняются определенные противоречия. Прозрачность и меры по укреплению доверия, пошаговый подход, много- и двусторонние компромиссы, обмен информацией и постоянные интенсивные дискуссии с широким участием НПО и экспертного сообщества не являются панацеей, но они представляют собой проверенный и безотказный рецепт. Сегодня мы здесь собрались, чтобы заставить этот рецепт работать. Я убежден, что в ходе сегодняшнего заседания мы уже внесли свой вклад в эту грандиозную задачу — конструктивный вклад, направленный на проработку этого крайне важного глобального вопроса. Теперь наша цель в том, чтобы продолжить этот позитивный процесс. Я надеюсь, что эта встреча станет лишь первым шагом в длительном системном процессе, который объединит усилия российских, западных и многих других экспертов и ответственных лиц, направленные на укрепление безопасности киберпространства и обеспечение беспрепятственного использования информационных технологий по всему миру.